IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Dodson et al.**	§	
	§	Group Art Unit: **2131**
Serial No. **10/631,066**	§	
	§	Examiner: **Revak, Christopher A.**
Filed: **July 31, 2003**	§	
	§	
For: **Method and Apparatus for Authenticated Network Address Allocation**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on August 1, 2007.

A fee of $510.00 is required for filing an Appeal Brief. Please charge this fee to Yee & Associates, P.C. Deposit Account No. 50-3157. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to Yee & Associates, P.C. Deposit Account No. 50-3157. A one-month extension of time is believed to be necessary. Please charge the $120.00 extension fee to Yee & Associates, P.C. Deposit Account No. 50-3157. No additional extension of time is believed to be necessary. If, however, an additional extension of time is required, the extension is requested and, I authorize the Commissioner to charge these additional fees which may be required to Yee & Associates, P.C. Deposit Account No. 50-3157.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, New York.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-23

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 2, 10, 16 and 23
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1, 3-9, 11-15 and 17-22
4. Claims allowed: none
5. Claims rejected: 1, 3-9, 11-15 and 17-22
6. Claims objected to: none

C. CLAIMS ON APPEAL

The claims on appeal are: 1, 3-9, 11-15 and 17-22

STATUS OF AMENDMENTS

No amendment after final rejection was filed for this case.

SUMMARY OF CLAIMED SUBJECT MATTER

Computers on a network typically have addresses, such as Internet Protocol (IP) addresses. In some cases, the addresses are static addresses, which may be permanently assigned to a computer. In other cases, the addresses may be automatically assigned to a computer when it logs on to a network, such as a Transmission Control Protocol (TCP)/IP network. With this type of network, a dynamic host configuration protocol (DHCP) server automatically assigns IP addresses to the client computers logging on to the network. This type of process is typically found on a server, but also may be implemented in other types of network devices, such as integrated services digital network (ISDN) routers and modem routers that allow multiple users to access the internet.

However, DHCP does not authenticate the identity of the clients before assigning the addresses. This DHCP protocol assumes that all of the clients on the network are allowed to obtain addresses from the server. The present invention provides a method, apparatus, and computer program product for providing addresses to clients. When a request is received from a client, a determination is made as to whether authentication information is present in the request. If it is present, the validity of this authentication information is verified. If the identity of the client is verified, a privileged address is provided to the client in response to the authentication information being authenticated.

A. CLAIM 1 - INDEPENDENT

Claim 1 is directed to a method in a data processing system for providing addresses to clients. A request is received from a client for an address (Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700). A determination is made as to whether authentication information is present in the request, and an authentication process is performed using the authentication information if the authentication information is present in the request (Specification page 11, lines 19-25; page 12, lines 6-14; page 15, lines 4-6; Figure 7, block 704). A determination is made as to whether the authentication information is authenticated, and in response to the authentication information being authenticated, a privileged address is provided to the client (Specification page 11, lines 25-29 and page 11, line 31 – page 12, line 5; Figure 7, blocks 706, 708 and 710). In response to the authentication information not being authenticated,

a standard address is provided to the client (Specification page 12, lines 17-19; Specification page 16, lines 9-11; Figure 7, block 722). Thus, one of two different types of addresses is provided back to a requesting client device depending upon whether the authentication information is authenticated or not.

B. CLAIM 7 – INDEPENDENT

Claim 7 is directed to a method in a data processing system for assigning addresses to clients. A request from a client for an address is received (Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700). A determination is made as to whether authentication information is present in the request, and if the authentication information is present in the request, a verification process is performed using the authentication information (Specification page 11, lines 19-25; page 12, lines 6-14; page 15, lines 4-6; Figure 7, block 704). A determination is made as to whether the authentication information is verified, and responsive to the authentication information being verified, an address is provided to the client (Specification page 12, lines 6-16; Figure 7, elements 706, 708 and 710). Responsive to the authentication information not being verified, the request is denied (Specification page 16, lines 15-18). The address is received by the client, where the address received by the client is included in an offer from a server that performed the verification process (Specification page 12, lines 24-28; page 14, lines 9-10; Figure 6, block 608). The client determines whether the offer is authentic, and responsive to the offer being authentic, the offer is accepted by the client (Specification page 12, lines 29-30; page 14, lines 10-14; Figure 6, blocks 612 and 614).

C. CLAIM 8 – INDEPENDENT

Claim 8 is directed to a data processing system for providing addresses to clients. The data processing system includes receiving means for receiving a request from a client for an address (Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700). The data processing system includes first determining means for determining whether authentication information is present in the request (Specification page 15, lines 4-6; Figure 7, block 704). The data processing system also includes performing means for performing an authentication process using the authentication information if the authentication information is present in the request (Specification page 15, lines 7-9; Figure 7, block 706), second determining means for

determining whether the authentication information is authenticated, and providing means, responsive to the authentication information being authenticated, for providing a privileged address to the client, where the privileged address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client (Specification page 11, lines 19-25; page 12, lines 6-16; page 15, lines 20-29; Figure 7, elements 708 and 710).

The equivalent structure for each of the means recited in Claim 8 (receiving means, first determining means, performing means, second determining means, and providing means) is described in the Specification at Specification page 6, line 28 – page 7, line 25 and depicted in Figure 2, element 200.

D. CLAIM 14 – INDEPENDENT

Claim 14 is directed to a data processing system for assigning addresses to clients. The data processing system includes receiving means for receiving a request from a client for an address (Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700). The data processing system includes determining means for determining whether authentication information is present in the request and performing means for performing an authentication process using the authentication information if the authentication information is present in the request (Specification page 11, lines 19-25; page 12, lines 6-14; page 15, lines 4-6; Figure 7, block 704). The data processing system includes determining means for determining whether the authentication information is authenticated and means, responsive to the authentication information being authenticated, for providing an address to the client (Specification page 12, lines 6-16; Figure 7, elements 706, 708 and 710). The data processing system includes denying means, responsive to the authentication information not being authenticated, for denying the request (Specification page 16, lines 15-18). The data processing system also includes means for receiving the address by the client, wherein the address received by the client is included in an offer (Specification page 12, lines 24-28; page 14, lines 9-10; Figure 6, block 608). The data processing system also includes means for determining, by the client, whether the offer is authentic and means, responsive to the offer being authentic, for accepting the offer by the client (Specification page 12, lines 29-30; page 14, lines 10-14; Figure 6, blocks 612 and 614).

The equivalent structure for the receiving means, determining means, performing means, determining means, providing means and denying means recited in Claim 14 is described in the Specification at Specification page 6, line 28 – page 7, line 25 and depicted in Figure 2, element 200. The equivalent structure for the means for receiving the address by the client, means for determining by the client, and means for accepting the offer by the client as recited in Claim 14 is described in the Specification at Specification page 8, line 8 – page 9, line 18 and depicted in Figure 3, element 300.

E. CLAIM 15 – INDEPENDENT

Claim 15 is directed to a computer program product encoded in a computer readable medium for providing addresses to clients when executed by a data processing system. The computer program product includes instructions for receiving a request from a client for an address (Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700). The computer program product includes instructions for determining whether authentication information is present in the request, and instructions for performing an authentication process using the authentication information if the authentication information is present in the request (Specification page 11, lines 19-25; page 12, lines 6-14; page 15, lines 4-6; Figure 7, block 704). The computer program product also includes instructions for determining whether the authentication information is authenticated, and instructions, responsive to the authentication information being authenticated, for providing a privileged address to the client (Specification page 11, lines 25-29 and page 11, line 31 – page 12, line 5; Figure 7, blocks 706, 708 and 710). The computer program product also includes instructions, responsive to the authentication information not being authenticated, for providing a standard address to the client (Specification page 12, lines 17-19; Specification page 16, lines 9-11; Figure 7, block 722). Thus, one of two different types of addresses is provided back to a requesting client device depending upon whether the authentication information is authenticated or not.

F. CLAIM 21 – INDEPENDENT

Claim 21 is directed to a computer program product in a data processing system for assigning addresses to clients when executed by the data processing system. The computer program product includes first instructions for receiving a request from a client for an address

(Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700). The computer program product includes second instructions for determining whether authentication information is present in the request and instructions for performing an authentication process using the authentication information if the authentication information is present in the request (Specification page 11, lines 19-25; page 12, lines 6-14; page 15, lines 4-6; Figure 7, block 704). The computer program product also includes instructions for determining whether the authentication information is authenticated and instructions, responsive to the authentication information being authenticated, for providing an address to the client (Specification page 11, lines 25-29 and page 11, line 31 – page 12, line 5; Figure 7, blocks 706, 708 and 710). The computer program product also includes sixth instructions, responsive to the authentication information not being authenticated, for denying the request (Specification page 16, lines 15-18). The computer program product also includes instructions for receiving the address by the client, where the address is included in an offer (Specification page 12, lines 24-28; page 14, lines 9-10; Figure 6, block 608). The computer program product also includes instructions for determining, by the client, whether the offer is authentic, and instructions, responsive to the offer being authentic, for accepting the offer by the client (Specification page 12, lines 29-30; page 14, lines 10-14; Figure 6, blocks 612 and 614).

G. CLAIM 22 – INDEPENDENT

Claim 22 is directed to a data processing system for providing addresses to clients. The data processing system comprises a bus system, a memory connected to the bus system, a communications adaptor connected to the bus system, and a processor unit connected to the bus system (Specification page 6, line 28 – page 7, line 25; Figure 2, element 200). The processor unit executes a set of instructions included in the memory to receive a request from a client for an address (Specification page 11, lines 18-19; page 15, lines 1-2; Figure 7, block 700), determine whether authentication information is present in the request (Specification page 15, lines 4-6; Figure 7, block 704); perform an authentication process using the authentication information if the authentication information is present in the request (Specification page 15, lines 7-9; Figure 7, block 706), determine whether the authentication information is authenticated, and provide a privileged address to the client in response to the authentication information being authenticated (Specification page 11, lines 25-29; page 11, line 31 – page 12, line 5; page 15, lines 20-29;

Figure 7, blocks 706, 708 and 710). The privileged address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client (Specification page 15, lines 29-32).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to review on appeal are as follows:

1. Whether Claims 15-21 are statutory under 35 U.S.C. § 101;

2. Whether Claims 1, 3-5, 11, 12, 15 and 17-19 are anticipated by Jin et al., U.S. Patent 6,311,275 under 35 U.S.C. § 102(b);

3. Whether Claims 6, 13 and 20 are obvious over Jin et al., U.S. Patent 6,311,275 under 35 U.S.C. § 103;

4. Whether Claims 7, 14 and 21 are obvious over Droms, RFC 2131 in view of Droms et. al., RFC 3118 under 35 U.S.C. § 103; and.

5. Whether Claims 8, 9 and 22 are obvious over Jin et al., U.S. Patent 6,311,275 in view of Bahl et al., U.S Patent 6,957,276 under 35 U.S.C. § 103.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 15-21)

Claims 15-21 stand rejected under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. This rejection is respectfully traversed.

A.1. Claims 15-20

With respect to Claims 15-20, per MPEP 2106(IV)(B)(1)(a), a claimed *computer-readable medium encoded with a data structure* defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and is thus statutory (see also *Lowry,* 32 F.3d at 1583-84, 32 USPQ2d at 1035). Claim 15 was previously amended to directly comply with the MPEP requirements. Specifically, Claim 15 recites "a computer program product *encoded in a computer readable medium for providing addresses to clients when executed by a data processing system*". Therefore, Claims 15-20 are statutory under 35 U.S.C. § 101[1].

A.2. Claim 21

With respect to Claim 21, the Examiner states in rejecting such claim that the claim is directed to software alone and should be amended to indicate that the computer program product is stored on computer readable storage/recording medium. Applicants note that Claim 21 recites that the computer program product *is in a data processing system* and thus such claim recites a specific apparatus (a "data processing system"). Therefore, such claim complies with 35 U.S.C. § 101 as this is an apparatus claim, which is either a machine or a manufacture (both of which are expressly enumerated categories of proper statutory subject matter under 35 U.S.C. § 101[2]).

---

[1] These claims are distinguishable from the signal claims found to be non-statutory subject matter in *In re Petrus A.C.M. Nuijten*, No. 2006-1371, Fed Cir. 2007 as those claims expressly recited "A signal" in the claims, whereas in the instant case the claims recite "a computer program product *encoded in a computer readable medium* for providing addresses to clients when executed by a data processing system" which is expressly acknowledged by both judicial case law and the USPTO's own MPEP rules as being directed to valid statutory subject matter under 35 U.S.C. § 101 (MPEP 2106(IV)(B)(1)(a)).

[2] 35 U.S.C. 101:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of

Accordingly, Claim 21 has been erroneously rejected under 35 U.S.C. § 101, as such claim expressly recites a data processing system.

B. GROUND OF REJECTION 2 (Claims 1, 3-5, 11, 12, 15 and 17-19)

Claims 1, 3-5, 11, 12, 15 and 17-19 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Jin et al., U.S. Patent 6,311,275.

As will be shown in detail below, the cited Jen reference teaches a traditional DHCP server that returns an IP address if the user is successfully authenticated. The primary issue in the rejection of Claim 1 is whether it is proper for the Examiner to ignore the word "privileged" from the "privileged address" terminology that is expressly recited in the claims. The Examiner acknowledges that claims are to be interpreted in the light of the Specification, but states that limitations from the Specification will not be read into the claims. In essence, the Examine is interpreting "privileged address" to be "address". Thus, not only is the Examiner refusing to interpret the claims in light of the Specification, but the Examiner takes the further step of ignoring specific terminology ('privileged') in the claim itself – which is clear error.

The Examiner is also impermissibly ignoring the "not authenticated" scenario recited in the claims, where another type of address is returned to the user in such a "not authenticated" scenario (i.e. a 'regular' address is returned in the "not authenticated" scenario versus a 'privileged' address that is returned in the "authenticated" scenario). The Examiner cites Jen's return of a dummy address to fit this scenario, but this dummy address is returned when the user *has been authenticated* (and we claim a different type of address is returned when the user *has not been authenticated*).

The Examiner is also erroneously providing a double-standard in the present claim rejection. In the 35 U.S.C. § 101 rejection, the Examiner goes to great lengths to read Specification limitations into the claims to establish that the program-product claims impermissibly cover transmission-type media, and yet in the 35 U.S.C. § 103 rejection the Examiner states that limitations from the Specification will not be read into the claims. So in one instance (35 USC 101 rejection), the Specification is being used to define/interpret the claim

---

matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the

terminology and in another instance (35 USC 101 rejection), the Specification is deliberately not being used to define/interpret the claim terminology.

For a prior art reference to anticipate in terms of 35 U.S.C. 102, *every element* of the claimed invention must be *identically shown* in a single reference. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990) (emphasis added by Applicants). Applicants will now show that every element recited in Claims 1, 3-5, 11, 12, 15 and 17-19 is not identically shown in a single reference, and thus these claims are not anticipated by the cited Jin reference.

B.1. Claims 1, 4, 5, 11, 12 and 15

With respect to Claim 1, it is urged that the cited reference does not teach the claimed feature of "responsive to the authentication information being authenticated, providing a privileged address to the client". As can be seen, a *privileged* address is provided to the client responsive to the authentication information being authenticated. The cited reference does not teach any type of privileged address. In rejecting this aspect of Claim 1, the Examiner cites Jin's teaching at col. 4, line 44 – col. 5, line 10 and col. 5, lines 22-24 as teaching this claimed feature. Applicants show that there, Jin states:

> "As described above, the user initiates a session on the network 5 by launching a dial-up application on his or her subscriber PC 1. The dial-up application prompts the user for user-name and password information, and contacts the NAS 2. The NAS 2 prepares an access-request packet containing the user-specified information, as well as information about the NAS client 2 itself. Instead of being delivered directly to the AAA Server 4, however, the access-request packet is first intercepted by the SSG Server 3, at step 200. Since the access-request packet contains username and password information, receipt of the access-request packet by the SSG Server 3 supplants the need for requiring the user to supply this information to the SSG Server 3 using a separate dashboard application. However, as described above, the SSG Server 3 still needs the user IP

conditions and requirements of this title.

address to complete the log-on procedure. The user IP address, however, has not yet been assigned, and extra steps must be taken before the SSG Server 3 can officially log the user on.

The SSG Server 3 forwards the access-request packet to the AAA Server 4 at step 202. The AAA Server 4 first authenticates the user by checking the data attributes in the access-request packet against its account database. The AAA Server 4 then responds to the access-request by issuing an access-reply packet back to the SSG Server 3 at step 204. If the user authentication check is successful, then the AAA Server 4 may assign an IP address to the user and include this IP address in the access-reply packet. The SSG server 3 then checks for an IP address in the access-reply packet. If the SSG Server 3 finds an IP address, then the SSG Server 3 can log the user on with the IP address provided by the AAA Server 4, and then forward the access-reply packet on to the NAS 2 immediately at step 206. Once the access-reply packet is received by the NAS 2, it may then log the user on as well, and the user session can begin." (col. 4, line 44 – col. 5, line 10)

and

"Upon receipt of the access-reply packet authorizing the user to access the network, **the NAS 2 assigns a genuine IP address to the user and logs the user on**." (col. 5, lines 22-24) (emphasis added by Applicants)

As can be seen, this passage describes the assignment of a *genuine* IP address, whereas in contrast Claim 1 recites providing a *privileged* address to the client. The term 'genuine' is not the same as the term 'privileged', and therefore every element recited in Claim 1 is not *identically shown in a single reference*. Accordingly, Claim 1 is not anticipated by the cited reference.

In addition, Claim 1 recites:

> "responsive to the authentication information *being authenticated*, providing a *privileged* address to the client; and responsive to the authentication information *not being authenticated*, providing a *standard* address to the client." (emphasis added by Appellants)

As can be seen, a *privileged* address is provided to the client responsive to authentication information *being authenticated*, and a *standard* address is provided to the client responsive to the authentication information *not being authenticated*. In rejecting this aspect of Claim 1 pertaining to the 'not being authenticated' scenario, the Examiner cites Jin's teaching at col. 5, lines 11-21 as teaching this 'not being authenticated' scenario. Applicants urge that there, and to the contrary, Jin states:

> *"If the AAA Server 4* ***authorizes*** *the user but does not assign an IP address*, then the SSG Server 3 can log the user on with a dummy temporary IP address. It then assigns the user an identification number that it inserts into the access-reply packet before forwarding the access-reply packet to the NAS 2 at step 206. The identification number is written as a special attribute in the access-reply packet, called a "class attribute" in the RADIUS protocol. The class attribute is read and stored by the NAS 2 and echoed back unchanged in subsequent packets. The temporary IP address can be used as an identification number." (emphasis added by Applicants)

As can be seen, this passage does not describe any type of scenario where authentication information has *not* been authenticated, but rather teaches just the opposite – *the user has in fact been authorized* ("If the AAA Server 4 *authorizes the user*"). Thus, it is shown that there are additional claimed features not identically shown in a single reference – and in particular the cited reference does not teach the claimed feature of "*responsive to the authentication*

information not being authenticated, providing a *standard address* to the client". Quite simply, the cited reference does not teach that one of two different types of addresses is provided back to a requesting client device depending upon whether the authentication information is authenticated or not.

Therefore, as every element recited in Claim 1 is not identically shown in a single reference, and in particular the reference does not teach (1) a privileged address, or (2) responsive to the authentication information *not being authenticated*, providing a standard address to the client, it is shown that Claim 1 is not anticipated by the cited reference[3].

B.2. Claim 3

Appellants initially show error in the rejection of Claim 3 for reasons given above with respect to Claim 1 (of which Claim 3 depends upon).

Further with respect to Claim 3, it is urged that the cited reference does not teach the claimed feature of "wherein the privileged address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client". As can be seen, per the expressly recited features of Claim 3, the privileged addressed that is returned back to the client is explicitly defined to be "a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client". In rejecting Claim 3, the Examiner states that this claimed feature is taught by Jin in that Jin teaches 'the address is an Internet Protocol address (col. 5, lines 1-3)'. Appellants urge error, as Claim 3 does not merely recite that the address is "an Internet Protocol address" as alleged by the Examiner to be taught by the cited reference. Rather, Claim 3 is directed to a particular type of Internet Protocol address - a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client. The cited Jin reference does not teach (or otherwise suggest) the particular type of IP address as expressly recited per the features of Claim 3, and thus it is further shown that Claim 3 has been

[3] For a prior art reference to anticipate in terms of 35 U.S.C. 102, *every element* of the claimed invention *must be identically shown* in a single reference. *In re Bond, supra.*

erroneously rejected under 35 U.S.C. § 102(b) as there are additional claimed features that are not identically shown in a single reference.

C. GROUND OF REJECTION 3 (Claims 6, 13 and 20)

Claims 6, 13 and 20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Jin et al., U.S. Patent 6,311,275.

C.1. Claims 6, 13 and 20

Appellants urge error in this rejection for similar reasons to those given above with respect to independent Claims 1, 8 and 15, respectively. Further, in rejecting such claim the Examiner alleges that the features recited in such claims are notoriously well-known, and thus obvious. Appellants urge that an allegation that something is 'notoriously well known' is not a valid basis for claim rejection under 35 U.S.C. § 103. As the Federal Circuit outlines in *Ruiz v. A.B. Chance Co.*, 357 F.3d 1270, 1275 (Fed. Cir. 2004), in making the assessment of differences between the prior art and the claimed subject matter, section 103 specifically requires consideration of the claimed invention "as a whole". Inventions typically are new combinations of existing principles or features. *Envtl. Designs, Ltd. V. Union Oil Co.*, 713 F.2d 693, 698 (Fed. Cir. 1983) (noting that "virtually all [inventions] are combinations of old elements"). The "as a whole" instruction in title 35 prevents evaluation of the invention part by part. *Ruiz*, 357 F.3d at 1275. Without this important requirement, an obviousness assessment might successfully break an invention into its component parts, then find a prior art reference corresponding to each component. *Id.* This line of reasoning would import hindsight into the obviousness determination by using the invention as a roadmap to find its prior art components. Further, this improper method would discount the value of combining various existing features or principles in a new way to achieve a new result – often the essence of invention. *Id.* Contrary to this reasoning, section 103 requires assessment of the invention as a whole. *Id.* This "as a whole" assessment of the invention requires a showing that an artisan of ordinary skill in the art at the time of the invention, confronted by the same problems as the inventor and with no knowledge of the claimed invention, would have selected the various elements from the prior art and combined them in the claimed manner, *Id.*, which is consistent with the factual inquiry dictated by *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966) and M.P.E.P 2141. In 1983, the late Judge

Howard Markey made the following observation in *W.L. Gore & Associates Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), which states the basic interest protected by this test—improper hindsight analysis of prior art:

> "To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher."

It is respectfully urged that when properly analyzing Claim 6 under the 'as a whole' analysis, there is no teaching or suggestion in any of the cited references of an authentication process determining whether the a digital certificate is (i) from a trusted authority and (ii) is valid as a part of conditionally providing either a privileged or standard address to a requesting client depending upon whether or not the digital certification is from a trusted authority and is valid, or not. Thus, the Examiner's 'notoriously well known' reasoning in rejecting Claim 6 is shown to be in clear error, as the claim is not being analyzed 'as a whole' (as described above), and thus Claim 6 has been erroneously rejected under 35 U.S.C. § 103 as there is no teaching or suggestion in the cited reference or any other art of record to modify such teachings in accordance with the missing claimed features recited in Claim 6.

D. GROUND OF REJECTION 4 (Claims 7, 14 and 21)

Claims 7, 14 and 21 stand rejected under 35 U.S.C. § 103 as being unpatentable over Droms, RFC 2131 in view of Droms et al. RFC 3118.

D.1. Claims 7, 14 and 21

Claim 7 includes two different occurrences of verification/authentication – a verification being performed as a part of providing an address to a client in response to a request for an address by such client ("performing a verification process using the authentication information"), and an authentication being performed at the client as a part of receiving the requested address in an offer ("receiving the address by the client, wherein the address received by the client is included in an offer from a server that performed the verification process; determining, by the

client, whether the offer is authentic; and responsive to the offer being authentic, accepting the offer by the client"). *In addition*, the server-side verification process is conditionally performed based upon whether authentication information is present in the client request for an address ("performing a verification process using the authentication information *if the authentication information is present in the request*"). It is respectfully submitted that neither of the cited Droms references teach/suggest a *server-side verification process that is conditionally performed* based upon whether authentication information is present in the client request for an address, where such conditional processing at the server triggers the providing of an address to the client ("responsive to the authentication information being verified, providing an address to the client").

In rejecting Claim 7, the Examiner provides no teaching or suggestion of the claimed feature of "performing a verification process using the authentication information *if the authentication information is present in the request*", and "*responsive to the authentication information being verified, providing an address to the client*". The Examiner merely alleges "RFC 3118 discloses that authentication occurs between a server and client in order to complete the DHCP process", citing Droms RFC 3118 page 4, section 1.4, step 5; page 6, section 5.3, and page 7, section 5.5.1. Appellants urge that the cited passage at Droms section 1.4 states that a client obtains configuration parameters such as a network address, and that a server returns configuration parameters to DHCP clients. This cited passage does not teach either one of the claimed features of "performing a verification process using the authentication information *if the authentication information is present in the request*", or "*responsive to the authentication information being verified, providing an address to the client*". As to the cited passage at section Droms 5.3, this passage describes *message authentication*, which is different from *entity verification* (Droms 3118 page 1, last paragraph of Section 1 Introduction). Importantly, there is no need or desire to include an address in such message authentication, and in fact there is no defined field to include such an address (Droms 3118 page 5, Section 5.2 Format, DHCPOFFER format, where a Secret ID and HMAC-MD5 are provided to the client in response to a client's DHCPDISCOVER request – which is used by the client to request authentication (Droms Section 5, Delayed authentication). This cited passage does not teach both of the claimed features of "performing a verification process using the authentication information *if the authentication information is present in the request*", and "*responsive to the authentication information being*

verified, providing an address to the client". Finally, as to the cited Droms 3118 passage at Section 5.5.1, such passage describes a client performing a validation test on any DHCPOFFER messages *that include authentication information.* There is no teaching or suggestion of any type of address being provided in such DHCPOFFER message, and as previously described such DHCPOFFER has not address field in it as it is used to provide authentication information back to the client that requested it (Droms page 6, Section 5.3). Thus, this cited passage does not teach both of the claimed features of "performing a verification process using the authentication information *if the authentication information is present in the request*", and "*responsive to the authentication information being verified, providing an address to the client*".

Therefore, while it may be true that Droms 3118 discloses 'that authentication occurs between a server and client' (as alleged by the Examiner in rejecting Claim 7), the particular handshake details recited in Claim 7 to accomplish authentication - including conditionally providing an address to the client in response to authentication information being verified - is not in fact taught or suggested by the cited references, as the combined teachings instead describe that *authentication information is returned to the client* in response to a client's request for authentication (Droms 3118, page 4, Section 5 Delayed Authentication and Section 5.2 Format).

These missing claimed features can also be seen in that Droms 2131 describes the return of an address in the 'ciaddr' field (which is not a field in a DHCPOFFER message), and this address is only returned when a client is in a BOUND, RENEW, or REBINDING state (Droms 2131 page 9, 'ciaddr' field description). This 'ciaddr' address field is not described as being used in any type of authentication processing in either of the cited references. It is therefore urged that Claim 7 has been erroneously rejected, in that the combined teachings of the cited references do not teach *both* the claimed steps of (i) "performing a verification process using the authentication information if the authentication information is present in the request", *and* "responsive to the authentication information being verified, providing an address to the client".

Thus it is urged that Claim 7 is not obvious in view of the cited references as there are missing claimed features that are not taught or suggested by the cited references.

E. GROUND OF REJECTION 5 (Claims 8, 9 and 22)

Claims 8, 9 and 22 stand rejected under 35 U.S.C. § 103 as being unpatentable over Jin et al., U.S. Patent 6,311,275 in view of Bahl et al., U.S Patent 6,957,276.

E.1. Claim 8, 9 and 22

With respect to Claim 8, it is urged such claim is not obvious in view of the cited references, as such references do not teach or suggest a means ('providing means') for *providing a static IP address to a client responsive to authentication information being authenticated* for similar reasons to those given above with respect to Claim 1 (as the newly cited reference to Bahl does not teach any type of *client* authentication (but rather only describes *server* authentication, as further described below), and therefore does not teach/suggest anything being provided – either a static IP address, as claimed, or any other thing – responsive to authentication information (that is *received from a client*) being authenticated). Instead, the only conditional processing described by Bahl's static address being provided to a client is *whether or not an IP address is set to DEPRECATED* (Bahl col. 10, lines 6-22; Figure 5, block 236; col. 9, lines 1-12).

While the newly cited Bahl reference describes authentication, such authentication is *done by a client to ensure that the server is authentic* (Bahl col. 4, lines 25-37; col. 14, lines 27-47). The teachings of such reference do not contemplate conditionally providing a static IP address *to a client* depending upon whether or not authentication information received from such client has been authenticated, as claimed. Thus, the teachings of Bahl do not overcome the teaching deficiencies identified above with respect to Claim 1 and the cited Jin reference.

In conclusion, Appellants have shown numerous and substantial error in the final rejection of all pending claims, and thus respectfully requests that the Board reverse such improper final rejection of all such claims.

/Wayne P. Bailey/
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for providing addresses to clients, the method comprising:

receiving a request from a client for an address;

determining whether authentication information is present in the request;

performing an authentication process using the authentication information if the authentication information is presenting the request;

determining whether the authentication information is authenticated;

responsive to the authentication information being authenticated, providing a privileged address to the client; and

responsive to the authentication information not being authenticated, providing a standard address to the client.

3. The method of claim 1, wherein the privileged address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client.

4. The method of claim 1, wherein the authentication information is at least one of a pass phrase or a digital certificate.

5. The method of claim 4, wherein the authentication information is the pass phrase and wherein the authentication process determines whether the pass phrase is a valid pass phrase.

6. The method of claim 4, wherein the authentication information is the digital certificate and wherein the authentication process determines whether the certificate is from a trusted authority and is valid.

7. A method in a data processing system for assigning addresses to clients, the method comprising:

receiving a request from a client for an address;

determining whether authentication information is present in the request;

performing a verification process using the authentication information if the authentication information is present in the request;

determining whether the authentication information is verified;

responsive to the authentication information being verified, providing an address to the client;

responsive to the authentication information not being verified, denying the request;

receiving the address by the client, wherein the address received by the client is included in an offer from a server that performed the verification process;

determining, by the client, whether the offer is authentic; and

responsive to the offer being authentic, accepting the offer by the client.

8. A data processing system for providing addresses to clients, the data processing system comprising:

receiving means for receiving a request from a client for an address;

first determining means for determining whether authentication information is present in the request;

performing means for performing an authentication process using the authentication information if the authentication information is presenting the request;

second determining means for determining whether the authentication information is authenticated; and

providing means, responsive to the authentication information being authenticated, for providing a privileged address to the client, wherein the privileged address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client.

9. The data processing system of claim 8 further comprising:

providing means, responsive to the authentication information not being authenticated, for providing a standard address to the client.

11. The data processing system of claim 8, wherein the authentication information is at least one of a pass phrase and a digital certificate.

12. The data processing system of claim 11, wherein the authentication information is the pass phrase and wherein the authentication process determines whether the pass phrase is a valid pass phrase.

13. The data processing system of claim 11, wherein the authentication information is the digital certificate and wherein the authentication process determines whether the certificate is from a trusted authority and is valid.

14. A data processing system for assigning addresses to clients, the data processing system comprising:

receiving means for receiving a request from a client for an address;

determining means for determining whether authentication information is present in the request;

performing means for performing an authentication process using the authentication information if the authentication information is present in the request;

determining means for determining whether the authentication information is authenticated;

providing means, responsive to the authentication information being authenticated, for providing an address to the client;

denying means, responsive to the authentication information not being authenticated, for denying the request;

means for receiving the address by the client, wherein the address received by the client is included in an offer from the providing means;

means for determining, by the client, whether the offer is authentic; and

means, responsive to the offer being authentic, for accepting the offer by the client.

15. A computer program product encoded in a computer readable medium for providing addresses to clients when executed by a data processing system, the computer program product comprising:

first instructions for receiving a request from a client for an address;

second instructions for determining whether authentication information is present in the request;

third instructions for performing an authentication process using the authentication information if the authentication information is presenting the request;

fourth instructions for determining whether the authentication information is authenticated;

fifth instructions, responsive to the authentication information being authenticated, for providing a privileged address to the client; and

sixth instructions, responsive to the authentication information not being authenticated, for providing a standard address to the client.

17. The computer program product of claim 15, wherein the address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client.

18. The computer program product of claim 15, wherein the authentication information is at least one of a pass phrase and a digital certificate.

19. The computer program product of claim 18, wherein the authentication information is the pass phrase and wherein the authentication process determines whether the pass phrase is a valid pass phrase.

20. The computer program product of claim 18, wherein the authentication information is the digital certificate and wherein the authentication process determines whether the certificate is from a trusted authority and is valid.

21. A computer program product in a data processing system for assigning addresses to clients when executed by the data processing system, said computer program product comprising:

first instructions for receiving a request from a client for an address;

second instructions for determining whether authentication information is present in the request;

third instructions for performing an authentication process using the authentication information if the authentication information is present in the request;

fourth instructions for determining whether the authentication information is authenticated;

fifth instructions, responsive to the authentication information being authenticated, for providing an address to the client;

sixth instructions, responsive to the authentication information not being authenticated, for denying the request;

seventh instructions for receiving the address by the client, wherein the address received by the client is included in an offer;

eight instructions for determining, by the client, whether the offer is authentic; and

ninth instructions, responsive to the offer being authentic, for accepting the offer by the client.

22. A data processing system for providing addresses to clients, the data processing system comprising:

a bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions;

a communications adaptor connected to the bus system; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to receive a request from a client for an address; determine whether authentication information is present in the request; perform an authentication process using the authentication information if the authentication information is presenting the request; determine whether the authentication information is authenticated; and provide a privileged address to the client in response to the authentication information being authenticated, wherein the privileged address is a static Internet Protocol address that is identical to a previous address that was previously provided to the client in response to a previously received request from the client.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.